REMARKS

Reconsideration and allowance of the subject application are respectfully requested.

The Examiner's attention is directed to commonly-assigned U.S. Patent Application of Smeets et al., Serial No. 10/533,120, filed on April 29, 2005, entitled "SECURE IMPLEMENTATION AND UTILIZATION OF DEVICE-SPECIFIC SECURITY DATA." Consideration is requested.

Regarding the Examiner's withdrawing of claims 63-78 as being drawn to a non-elected species, Applicants respectfully point out that should generic claim 44 be found allowable than all non-elected species claims should be allowed as well.

Claims 44, 46-59, and 61 stand rejected under 35 USC §103(a) as being unpatentable based on a Wireless Identity Module protocol document referred to by the Examiner as WIM in view of Brown (5537474). This rejection is respectfully traversed.

Applicants' representative appreciates the courtesies extended by the Examiner during the interview conducted on July 23, 2009. As requested by the Examiner, claim 44 is amended to further clarify the distinctions over WIM and Brown. Non-limiting example support for the amendments may be found at page 14, lines 8-11, page 15, lines 3-5 and 17-18, and page 18, lines 25-29. The latter text at page 18, lines 25-29 describes redirection of commands to the cooperating application which, thereafter, may request that AKA processing at the AKA module fulfill security policy constraints coded in the cooperating application.

The WIM reference describes a tamper-resistant security device with a memory for storing user credentials like a security key and an AKA-module for performing AKA processing

with the security key. WIM defines an interface between part of a WAP client device and the tamper-resistant security device, i.e., WIM defines an **external** interface to the security device. Page 63 of the WIM-document discloses a card (mapped to a tamper-resistant security device) incorporating a WIM-application and other applications so that these applications are protected and executed in a tamper-resistant environment. But there is no disclosure in WIM of an **internal** interface between the other applications or the WIM-application and the AKA-module. Input to and output from the WIM-application and the other applications are directed over the external interface to the tamper-resistant security device for processing by the WIM-application or other applications.

Brown teaches a method and apparatus for authenticating a roaming subscriber. A subscriber receives a challenge that is in a format of a local authentication protocol and determines whether the local authentication protocol is the subscriber's home system authentication protocol. If it is not, the subscriber converts the challenge into a format (bit length) compatible with its home system authentication protocol and processes the converted challenge with the subscriber's secret key and authentication algorithm into an authentication response. The authentication response is converted to be compatible with the local authentication protocol and transmitted to a local system communication unit. The challenge and response is then forwarded to the subscriber's home system for similar conversion and processing, and the subscriber's response is compared against a home system generated response. Basically, Brown performs necessary conversions between the protocols but does not disclose or suggest cooperative processing within a tamper proof module like a SIM between an AKA module and an application that are both implemented within the tamper proof module.

The claimed application interface internal to the tamper-resistant device is for communication internally between an AKA-module and a cooperating application that performs enhanced security processing. The Examiner's attention is directed to the non-limiting example embodiments shown in Figures 3 and 4, where in addition to the external ME-SIM interface, there is an internal interface between the cooperating application and the AKA module for enhanced pre- or post-security processing of at least one AKA-related parameter.

Although a SIM could be loaded with an application that is completely independent of the AKA processing module, neither WIM nor Brown teach the claimed internal interface that allows cooperative processing between such an application and the AKA module so that the cooperating application selectively performs the claimed enhanced security processing in conjunction with the AKA module within the tamper-resistant security device, as recited in claim 44.

The Examiner admits that WIM does not teach a communications interface for external communication and an application interface internal to the tamper resistant security device for interfacing the AKA module and the cooperating application. The Examiner refers to the radio communication interface 110/120 in Brown as teaching the claimed external interface. Applicants submit that this mapping is not applicable because the radio interface is not with the tamper resistant security device 116 but instead with a radio unit at the terminal 110.

Regarding the claimed internal interface, the Examiner refers to col. 3, lines 48-58 in Brown. But this text simply describes typical security card functionality that performs authentication processing. There is no mention of the claimed "cooperating application, contained within the tamper-resistant security device and having been given access rights to

access the AKA module, configured to selectively receive the one or more AKA process commands and selectively provide enhanced security processing of the one or more AKA process commands." Although there is an internal interface between a memory and processor in a SIM used to execute authentication algorithms, that memory and processor used for AKA-processing are pre-manufactured and can not be changed during operation of the security device when installed in a user device. In contrast, the technology in claim 44 allows loading of a cooperating application into the security device over an external interface during its normal operation when installed in a user device. The loaded application communicates over the claimed internal interface with the AKA-module for selectively providing enhanced AKA processing. Brown's security device lacks this internal interface and selective enhanced AKA processing provided by a cooperating application. Any loaded application can only execute without any linkage to or dependence upon the AKA-module.

Regarding claims 51 and 56, Applicants cannot find any teaching in WIM or Brown of detecting security conditions and routing an AKA request either directly to the AKA module or to the cooperating application depending on the detected conditions.

Given the deficiencies noted with respect to the primary references, there is no need to address the rejections of dependent claim 60 and 62 based upon WIM and Brown in view of tertiary references.

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100